

September 2008

legal alert



New York Laws Affecting Custodians of Patient Information

Effective January 1, 2008, New York adopted a new law, General Business Law §399-dd, that regulates how you, as a custodian of patient information, must deal with Social Security numbers (SSNs) of your patients.

First, you may not intentionally disclose SSNs to the general public.

Second, in order to reduce the risks of inadvertent disclosure, the statute also prohibits you from doing certain things. Among them are the following: printing SSNs on cards required to be presented at the time of service; transmitting SSNs over the internet unless encrypted or transmitted over a secure connection; and entering SSNs on a website unless accompanied by a password or other unique identifier or authentication method. In addition, you may not print SSNs on materials you mail to your patients, unless you are required to do so by state or federal law or some other exception included in the statute. However, under no circumstances may you mail SSNs on postcards or in any other manner in which the SSNs are visible without opening the envelope.

Finally, you must adopt measures to assure that only your personnel who have a “need to know” the SSNs of your patients for legitimate business purposes have access to them.

There are very stiff penalties for failure to comply with this statute – up to \$100,000 for the first violation and up to \$250,000 for the second and subsequent violations. The Attorney General may also investigate the circumstances in which violations of this law occurred and seek an order from the court for restitution on behalf of patients whose SSNs have been improperly used or disclosed.

We recommend that you review all of your business practices, forms and other materials to determine how, when and by whom patient SSNs are accessed, transmitted or printed with an eye to eliminating any unnecessary use or appearance of SSNs.

Section 399-dd also provides additional protection to patients should their SSNs be included in any personal or private information compromised as a result of theft, loss of computers, data storage media, or paper records or system hacking. The opportunities for personal or private information about your patients (and employees, for that matter) to fall into the wrong hands are almost endless. A slightly older statute, General Business Law §899-aa, adopted in 2005, governs if something like this happens.

Section 899-aa imposes very specific obligations if your patients’ “personal information” or “private information” may have been disclosed in an unauthorized manner. Note that these obligations arise even if it is only a possibility that these data were compromised. Unless you know for a fact that patient “personal

information” or “private information” was not disclosed, you must comply with this statute. SSNs are included in the definition of “private information” under this statute.

Under Section 899-aa, you are required to notify the Attorney General if such an event occurs. An example of such an event is the theft of a laptop containing patient information. As a result, the Attorney General may begin an investigation of the incident, alerted by your notice.

Under Section §899-aa, the first thing you must do is notify the potentially affected patients that their “personal” and “private” information has been or may have been accessed by an unauthorized person. The notice must be made as quickly as possible, consistent with the needs of law enforcement personnel in conducting any investigation of possible criminal activity that lead to the breach. Your notice must tell your patients what items of personal and private information may have been improperly accessed.

You can give your notice in several ways: in writing, by email or by telephone. However, you may only use email if you have consent from your patients to communicate with them in that medium. If the notice is given by telephone, we recommend that callers be provided a script to follow. In addition, the callers must maintain a log of all notification calls they make.

If email or telephone notice is not possible or feasible, we recommend that your notice be given in the form of a letter, mailed via regular US mail. The letter should describe as completely as possible what is known about how the patient information may have been put at risk.

You may want to advise affected patients that there are steps they can take to protect their identities. The Attorney General’s Office has a brochure on its website that you may want to include with your notice. That website is www.oag.state.ny.us/consumer/tips/identity_theft.pdf.

Finally, the notice must include information on how your patients can contact you. We can help you with suggestions on how best to deal with this requirement, depending upon the nature and scope of the problem.

If the information that was compromised was of a particularly sensitive nature or includes SSNs, or if the security breach may have occurred as a result of human error or negligence on the part of your personnel, we strongly recommend you consider engaging a public relations consulting firm to advise you on how to handle patient and press inquiries.

As mentioned above, Section 899-aa requires that you notify the Attorney General, as well as the Consumer Protection Board and the State Office of Cyber Security and Critical Infrastructure Coordination, of the incident. The latter agency has developed a form to be used for this notice, which includes instructions on how to deliver it to these agencies. You can find this form at the CSCIC website at www.cscic.state.ny.us/security/securitybreach/.

We recommend that you contact your attorney to review the proposed patient notice to be sure it meets the statutory requirements and promptly notify your general liability insurance carrier of the incident. We would be happy to assist you should you find yourself in this unfortunate but all too common situation.

If you have questions concerning this Legal Alert, you may contact Helen Zamboni at (585) 258-2884, or by e-mail at hzamboni@underbergkessler.com.